



Jaime Merced  
Center for Assured Software  
National Security Agency

# Source Code Analysis Tool Evaluation

# Outline

- Overview of the project
- Description of the test suite
- Evaluation results

# About the project...

- Measure the accuracy and soundness of static analysis tools for C, C++, and Java source code

# Evaluating Static Analysis Tools

- Natural code
- Artificial code

# Artificial Test Cases

- Test cases contain a coding flaws and one or more fixes to the flaw

# Example of a Test Case

```
void CWE134_Uncontrolled_Format_String__scanf_to_printf_01_bad()
{
    char buf[SRC_NO_NTZ_SZ + 1];
    if (scanf(FMT_STR, buf) == 1)
    {
        /* FLAW: buf (obtained from scanf) is
           passed as the format string to printf */
        printf(buf);
    }
}
```

# Example of a Test Case (cont'd)

```
static void good1() {
    /* FIX: Use a static string for a format string */
    printf("good1\n");
}

static void good2() {
    /* FIX: Use a variable derived from a static string
       for a format string */
    char * s = "good2";
    printf(s);
}

static void good3() {
    char buf[SRC_NO_NTZ_SZ + 1];
    if (scanf(FMT_STR, buf) == 1)
    {
        /* FIX: Use %s as a format string and
           pass buf as an argument */
        printf("%s", buf);
    }
}
```

# Example of a Test Case (cont'd)

```
static void good1() {
    /* FIX: Use a static string for a format string */
    printf("good1\n")
}

static void good2() {
    /* FIX: Use a variable derived from a static string
       for a format string */
    char * s = "good2";
    printf(s);
}

static void good3() {
    char buf[SRC_NO_NTZ_SZ + 1];
    if (scanf(FMT_STR, buf) == 1)
    {
        /* FIX: Use %s as a format string and
           pass buf as an argument */
        printf("%s", buf);
    }
}
```

# Example of a Test Case (cont'd)

```
static void good1() {
    /* FIX: Use a static string for a format string */
    printf("good1\n")
}

static void good2() {
    /* FIX: Use a variable derived from a static string
       for a format string */
    char * s = "good2";
    printf(s);
}

static void good3() {
    char buf[SRC_NO_NTZ_SZ + 1];
    if (scanf(FMT_STR, buf) == 1)
    {
        /* FIX: Use %s as a format string and
           pass buf as an argument */
        printf("%s", buf);
    }
}
```

# Two Types of Test Cases

- Breadth of analysis
- Depth of analysis

# Breadth of Analysis

`cin` →  
`printf`

`read` →  
`printf`

`getc` →  
`printf`

`scanf` →    `scanf` →  
    `syslog`    `fprintf`    `sprintf`    `vprintf`    `printf`    `vfprintf`    `vsprintf`    `snprintf`    `vsnprintf`

`fscanf` →  
`printf`

`gets` →  
`printf`

`fgets` →  
`printf`

# Size of Test Case Suite

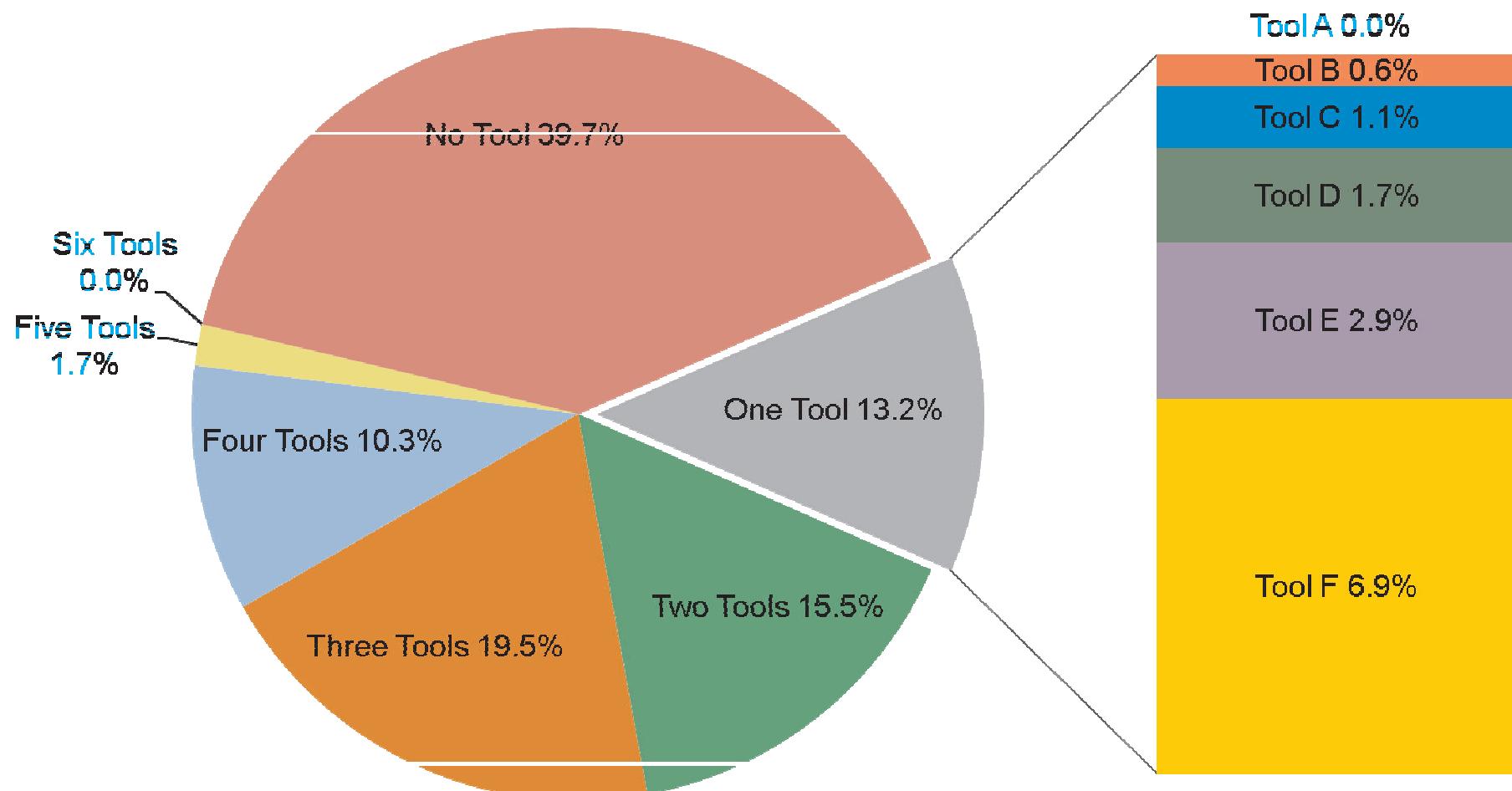
		# Test Cases	# CWEs Covered
C/C++	“Breadth”	210	103
	“Depth”	201	10
	All C/C++	411	103
Java	“Breadth”	177	112
	“Depth”	183	11
	All Java	360	112
	All	771	175

# Tools Evaluated

Tool	C/C++	Java
Coverity Prevent 4.3	✓	✓
FindBugs 1.3.7		✓
Fortify SCA 5.2	✓	✓
GrammaTech CodeSonar 3.2	✓	
Klocwork Insight 8.1	✓	✓
Ounce Labs Ounce 6	✓	✓
PMD 4.2.5		✓

# Evaluation Results

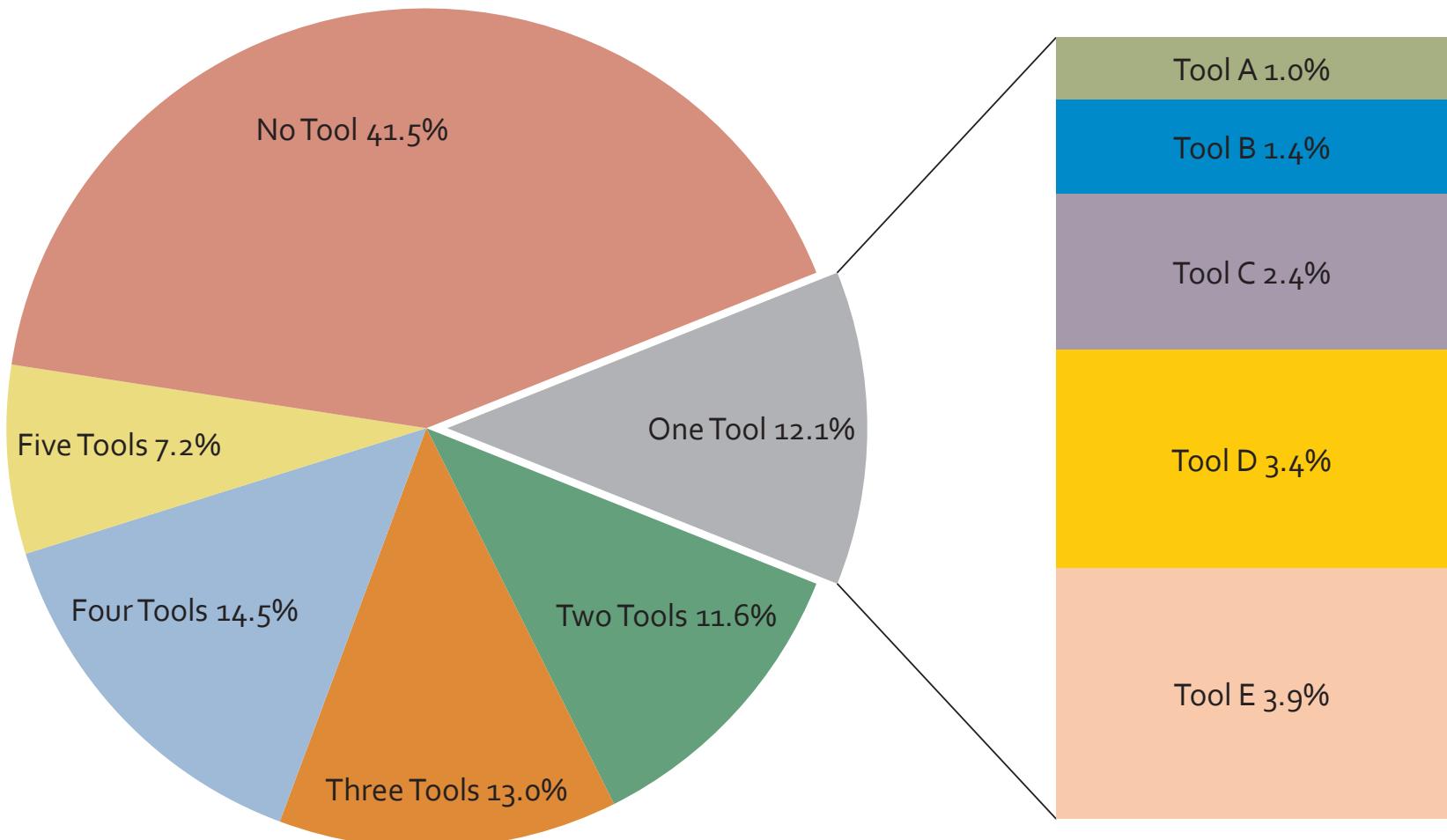
# Java “Breadth” Test Case Coverage



## Examples of Missed Test Cases (Java)

- CWE 369-Divide by zero
- CWE 482-Comparing instead of assigning
- CWE 484-Omitted break statement in switch
- CWE 606-Unchecked input for loop condition
- CWE 674-Uncontrolled recursion

# C/C++ “Breadth” Test Case Coverage



## Examples of Missed Test Cases (C/C++)

- CWE 190-Integer overflow or wraparound
- CWE 248-Uncaught exception
- CWE 374-Mutable objects passed by reference
- CWE 397-Declaration of throws for generic exception
- CWE 588-Attempt to access child of a non-structure pointer
- CWE 674-Uncontrolled recursion

# Summary

- Used artificial code to evaluate static analysis tools
- Evaluated 6 tools for Java
- Evaluated 5 tools for C/C++
- Results
  - Java
  - C/C++

# *Questions?*

## *Source Code Analysis Tool Evaluation*

Jaime Merced  
Center for Assured Software  
National Security Agency